OCIO

Building a Solid Security Foundation

Brief to Management Council

September XX, 2001

System Security Plan Review

Overview

A System Security Plan provides an overview of the security requirements of a system and describes the controls in place or planned for meeting those requirements. System Security Plans delineate responsibilities and expected behavior of all individuals who access the system.[1]

The National Institute of Standards and Technology (NIST) issued Special Publication (SP) 800-18 titled, "*Guide for Developing Security Plans for Information Technology Systems*" in December 1998. This guideline is used for documenting the security process, procedures and controls for Major Applications and General Support Systems.

A security plan will contain the buzzwords such as Intrusion Detection, Firewall, Encryption, Integrity, Identification, Contingency Plan, Audit, A-130, Risk Assessment, Rules of Behavior, and Personnel Security.

A completed, approved and updated SSP is used during reviews conducted for compliance with OBM A-130 Appendix III and FISCAM SP 2-1 or assessments conducted by the General Accounting Office (GAO) and Investigator General (IG).

System Security Plans are the founding document for a Certification and Accreditation (C&A) and without a SSP no form of a C&A is obtainable.

[1] NIST Self-Assessment Guide for IT Systems, Section 4.1.5

GISRA Review

GISRA

SFA has just responded to the 2001 GISRA assessment from GAO.

This assessment has found the following:

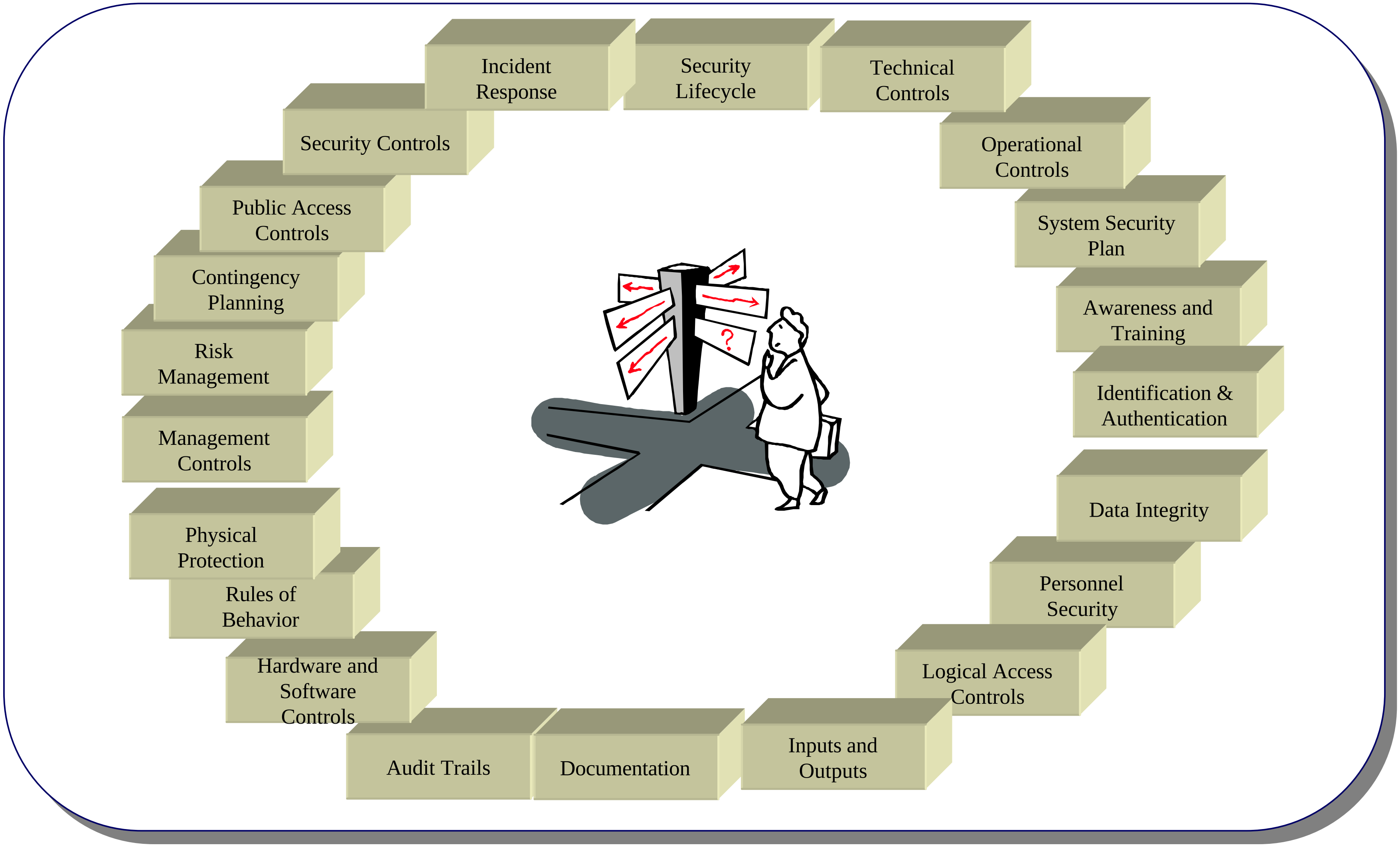
Pros

- VDC
- SDLC

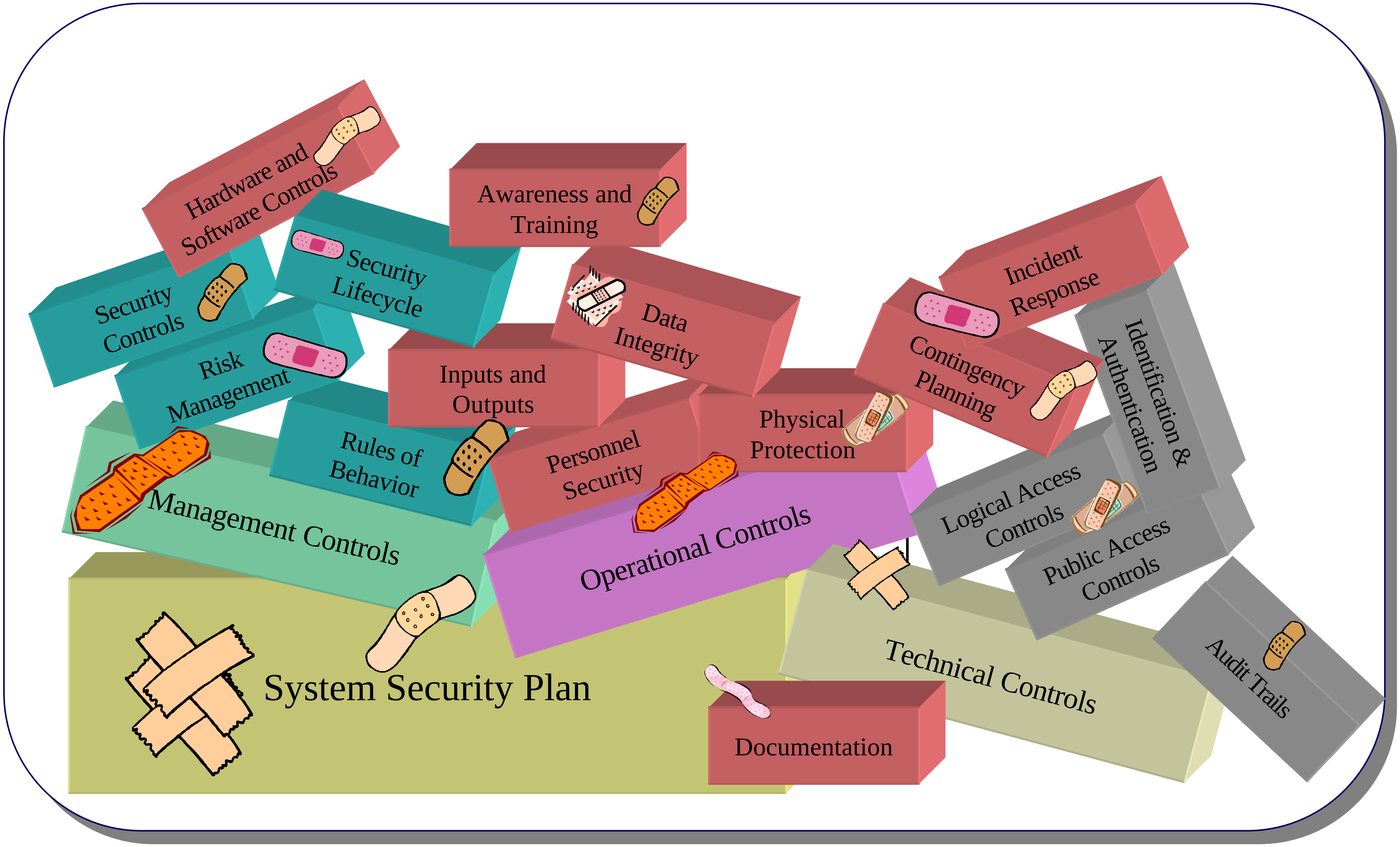
Cons

- Personnel Security
- SDLC

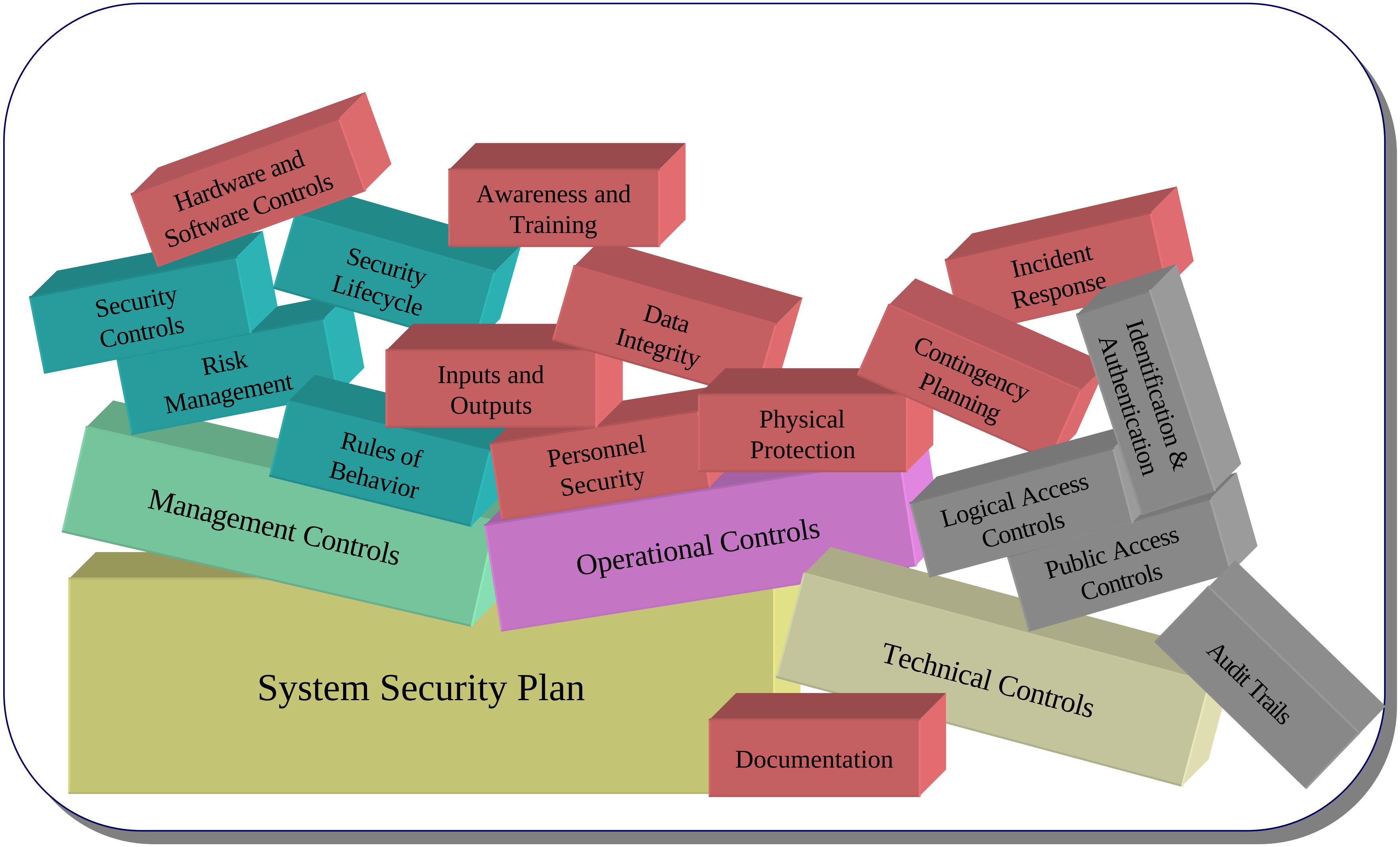
Where Do We Begin?



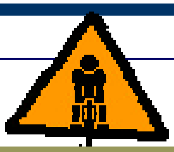
Typical Security Implementation



The Foundation Is . . .



What does a security plan do for your system?



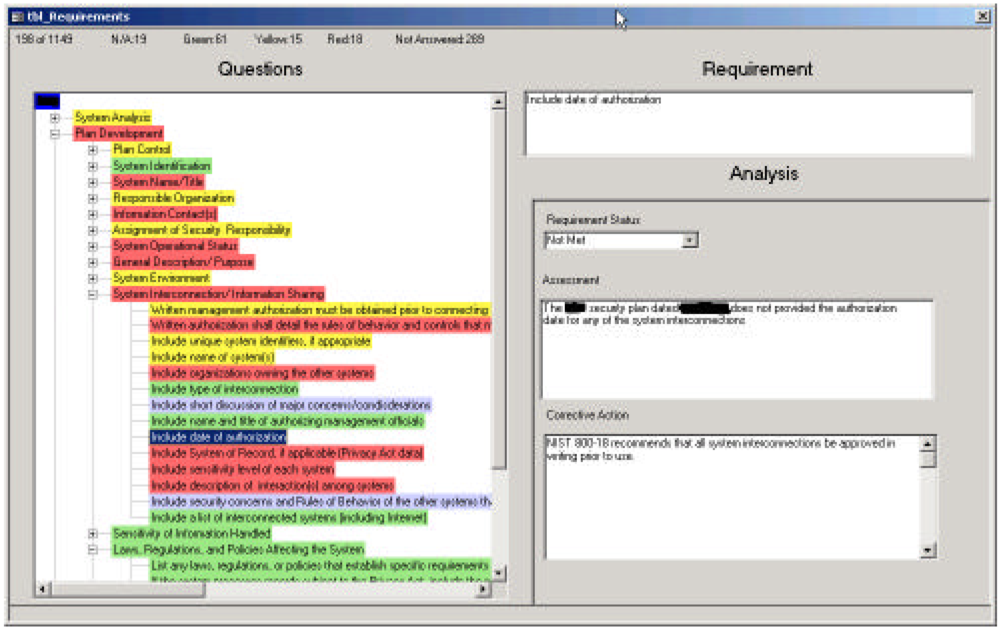
A System Security Plan should

- Ask all the questions about a system’s security and privacy challenges,
- Answer and document a system’s security and privacy procedures, and
- Provide a record of management decisions to limit risk.

Improving SFA Security Plans

This summer, the Mod Partner team received and analyzed three security plans and compared them to NIST 800-18.

An existing tool was customized for assessing security plans and recommended corrective action plans were prepared.



198 of 1149 N/A:19 Green:61 Yellow:15 Red:18 Not Answered:289

Questions

[redacted]
- System Analysis
- Plan Development
  - Plan Control
  - System Identification
  - System Name/Title
  - Responsible Organization
  - Information Contact(s)
  - Assignment of Security Responsibility
  - System Operational Status
  - General Description/ Purpose
  - System Environment
  - System Interconnection/ Information Sharing
    - Written management authorization must be obtained prior to connecting
    - Written authorization shall detail the rules of behavior and controls that n
    - Include unique system identifiers, if appropriate
    - Include name of system(s)
    - Include organizations owning the other systems
    - Include type of interconnection
    - Include short discussion of major concerns/considerations
    - Include name and title of authorizing management officials
    - Include date of authorization
    - Include System of Record, if applicable (Privacy Act data)
    - Include sensitivity level of each system
    - Include description of interaction(s) among systems
    - Include security concerns and Rules of Behavior of the other systems th
    - Include a list of interconnected systems (including Internet)
  - Sensitivity of Information Handled
  - Laws, Regulations, and Policies Affecting the System
    - List any laws, regulations, or policies that establish specific requirements

Requirement

Include date of authorization

Analysis

Requirement Status: Not Met

Assessment: The [redacted] security plan dated [redacted] does not provided the authorization date for any of the system interconnections.

Corrective Action: NIST 800-18 recommends that all system interconnections be approved in writing prior to use.

Security Plan Review Summary

The analysis of the security plans reveals the following:

	Plan 1	Plan 2	Plan 3
Is the plan in NIST 800-18 template?	NO	YES	YES
Is the plan's context correct?	NO	YES	NO
Does the plan include all appendices?	NO	NO	NO
Overall Score	35%	72%	55%

Recommendations

- For each of the three security plans reviewed, each system owner should update their SSP to reflect the review findings.
- The security plan review effort should continue to expand SFA's understanding of its system's risks and be aware of the controls in place to mitigate those risks.
- A training session should be conducted so all SSOs are familiar with NIST's guidance and can implement 800-18 accurately.